

**REMARKS**

The currently pending claims are independent claims 29 and 30. The claims are addressed to a solution of the problem of how a mobile station can authenticate itself to a new network B, taking advantage of the circumstances that: (i) the mobile station is already authenticated to old network A, and (ii) there exists a secure channel for communication between networks A and B.

Briefly, the solution as recited in the claims involves the mobile station identifying itself in a request to network B. Network B forwards the mobile's ID (such as the IMSI) to Network A together with an authentication key (such as SSD). Network A forwards the authentication key to the mobile station under the protection of an encryption key that has been established between Network A and the mobile station. The mobile station generates an authentication signature and sends it to Network A for forwarding to Network B. The authentication signature is generated from the mobile ID and the authentication key. For example, the authentication signature might be  $(\text{IMSI})_{\text{SSD}}$ , i.e., the IMSI encrypted by SSD. When Network B receives the authentication signature, it decides whether to accept it. If the authentication signature is accepted, the mobile station can enter into communication with Network B.

In the previous office action, the Examiner objected that the claims were incomplete as to certain features on which Applicants had based their arguments for patentability over the cited references. In the current amendment, certain features have been added to the claims. Specifically, the claims have been amended to include explicit recitations involving the active participation of the mobile station in communicating with Network A and in sending its identifier to Network B. These features are supported by the Specification at least at page 4, lines 14-31. Accordingly, it is submitted that the claim amendments introduce no new matter to the application.

Applicants submit that as amended, the claims fully support the remarks that Applicants previously submitted in support of the patentability of the claims over the cited art. Below, further arguments will be presented. To facilitate comparison between the present invention and the cited art, a uniform terminology will be adopted. In

accordance therewith, two entities, labeled X and Y, are seeking to establish communication with each other, with the help of a trusted agent Z.

In Marvit, Z provides an encryption code to X and a decryption code to Y. X uses the encryption code to send an encrypted message to Y. Y uses the decryption code to decrypt the message.

In Burrows at page 18, Z is a source of a key K for communication between X and Y. Z distributes the key K directly to X under the protection of a further key  $K_{XZ}$ . Z distributes the key K indirectly to Y; that is, Z encrypts K with the further key  $K_{YZ}$ , encrypts the result with the key  $K_{XZ}$ , and sends the resulting message to X. X decrypts the message with respect to  $K_{XZ}$  and forwards the result to Y.

Y then performs a “nonce handshake” with X to assure that X is currently present. That is, Y sends a number N to X and X returns a function of the number N to Y, both messages being under protection of the key K.

In Burrows at page 25, X is the source of the key K for communication between X and Y. The trusted agent Z is used to forward K from X to Y. The key K goes from X to Z under the protection of  $K_{XZ}$ , and then it goes from Z to Y under the protection of  $K_{YZ}$ .

It is important to note that all of the above scenarios involve pure key distribution. Not a single one of the above scenarios has an entity generating an authentication signature from an identifier and from shared secret data. Much less, then, is there any suggestion of using the trusted agent to help in the generation and transmission of an authentication signature.

Although the nonce handshake might *arguendo* be compared to authentication, it does not prove X’s identity but rather establishes that X is there now. In any event, N is not a key, and it is not combined with X’s ID. Moreover, the agent Z does not participate in the nonce handshake.

By contrast, the current claims will describe the following scenario if for purposes of argument SSD is considered to be a key, referred to here for consistency as “K”:

- (i) X sends its ID directly to Y.
- (ii) Y sends key K to Z for forwarding to X.
- (iii) X encrypts the ID with K to generate an authentication signature.

(iv) X then uses Z to forward the authentication signature to Y.

(In the terminology adopted in the claims, X is the mobile station, Y is Network B, and the trusted agent Z is Network A. As noted, K is SSD.)

Applicants wish to earnestly point out that of the above four steps, only (ii) relates to key distribution, and that this is so only in the limited sense that SSD functions as an encryption key in the algorithm which generates the authentication signature. (Thus, SSD is not being used to encrypt messages, but rather just to generate the authentication signature.) On the other hand, (i), (iii), and (iv) relate not to key distribution, but instead to generation of an authentication signature. As noted, neither Marvit nor the two sections of Burrows cited by the Examiner relate to generation of an authentication signature. Much less, then, do they so much as suggest the combination of steps in which the mobile station identifies itself directly to the new network, but uses the old network as a trusted agent for delivering SSD to the mobile from the new network and delivering the authentication signature from the mobile to the new network.

Even if the references were combined, they would still fail to suggest the claimed invention, because they would still lack any suggestion regarding generation and delivery of an authentication signature in the manner described above.

Moreover, there is no motivation to combine Marvit with Burrows at page 18 or Burrows at page 25, because Marvit teaches in a direction contradictory to the cited sections of Burrows. That is, Burrows at both page 18 and page 25 teaches a key distribution method whose outcome is that X and Y both possess the same key for communicating with each other. If this were the case, there would be no need for one party to obtain an encryption key, and the other party to obtain a decryption key, on a message-by-message basis as taught by Marvit.

Furthermore, Burrows at page 18 teaches that the trusted agent Z communicates directly only with X. This contradicts Marvit, where the trusted agent (i.e., the key repository) communicates directly with both parties.

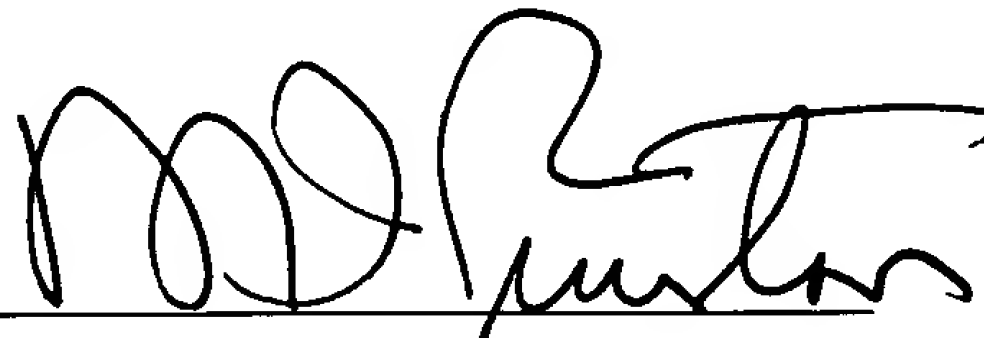
Still further, Burrows at page 25 teaches that X is the source of the key, and the trusted agent Z merely forwards the key to Y. This contradicts Marvit, where the trusted agent is the source of the keys.

**Serial No. 09/662580**

For all of the above reasons, it is respectfully submitted that claims 29 and 30, as amended, are patentable over the cited art under the standard of 35 USC §103. Allowance of the same is respectfully solicited.

Respectfully submitted,

**Douglas N. Knisely  
Robert Jerrold Marks  
Semyon B. Mizikovsky**

By 

**Martin I. Finston  
Attorney for the Applicant  
Reg. No. 31,613  
(973)-386-3147**

Date: Oct. 18 2005

**Docket Administrator (Room 3J-219)  
Lucent Technologies Inc.  
101 Crawfords Corner Road  
Holmdel, NJ 07733-3030**